UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

CARIN DICKMEYER and **JOEL BONNETT**, individually and on behalf of all other similarly situated, Plaintiffs, v. **PROGRESS SOFTWARE CORPORATION**, Defendant.	CASE NO._____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **Judge Allison D. Burroughs**

CLASS ACTION COMPLAINT

1. Plaintiffs JOEL BONNETT and CARIN DICKMEYER ("Plaintiffs"), individually and on behalf of all others similarly situated, brings this action against Defendant Progress Software Corporation ("Progress") or ("Defendant"). Plaintiffs allege the following based on personal knowledge as to their own acts and on the investigation conducted by their counsel as to all other allegations.

NATURE OF THE ACTION

2. This proposed Class Action is brought by individuals, including consumers, whose personal data was accessed and exposed by an unauthorized third-party in a data breach concerning Progress's MOVEit Transfer and MOVEit Cloud software ("Class members"), which Progress first learned of on May 28, 2023, reported to customers on May 30, 2023, and reported to the SEC and its investors on June 5, 2023 (the "Data Breach"). *See Form 8-K filed 6/5/2023*, https://investors.progress.com/static-files/e8a76c9d-310a-4762-8853-e92a1952d6a4 (last visited

Oct. 8, 2023); *see also*, *Form 10-Q filed 7/7/2023*, https://investors.progress.com/static-files/90ee1d91-3191-40f0-97dd-e94d6aa26f7d at 20-21, 32-33 (last visited Oct. 8, 2023).

3. Progress sells MOVEit Transfer, "On-Premises Managed File Transfer (MFT) software designed for "for secure collaboration and automated file transfers of sensitive data in compliance with SLAs, governance and data protection regulations" including "PCI, HIPAA, CCPA/CPRA and GDPR, SOC 2 type2, ISO 27001, SOX, BAEL I/II/III, FIPS, FISMA, GLBA, FFIECT, [and] ITAR," which can "[a]ssure the secure and compliant transfer of protected data" *See MOVEit Transfer,* https://www.progress.com/moveit/moveit-transfer (last visited Oct. 10, 2023).

4. Progress also sells "MOVEit Cloud: Managed File Transfer as-a-Service" which it describes as a "trusted and proven SaaS solution," that "provides full security, reliability and compliance with the convenience of a cloud-based service" that has been "auditor-certified PCI, SOC 2 type 2, and HIPAA compliant and ensure CCPA/CPRA and GDPR readiness in external file transfer activities involving personal data" allowing customers to enjoy "best in class security…." *Id.*

5. On May 31, 2023, Progress posted an article on its community website alerting its customers that:

> Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362), last modified June 21, 2023, https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (last visited Oct. 10, 2023).

6. On June 4, 2023, Microsoft Corp., an information technology company, attributed "attacks exploiting the CVE-2023-34362 MOVEit Transfer 0-day vulnerability to Lace Tempest, known for ransomware operations & running the Clop extortion site. The threat actor has used similar vulnerabilities in the past to steal data & extort victims." https://twitter.com/MsftSecIntel/status/1665537730946670595 (last visited Oct. 11, 2023).

7. On June 5, 2023, Progress informed its investors that on May 28, 2023, the:

> MOVEit technical support team at Progress […] received an initial customer support call indicating unusual activity within their MOVEit Transfer instance. An investigative team was mobilized and discovered a zero-day vulnerability in MOVEit Transfer. The investigative team determined that the vulnerability could provide for unauthorized escalated privileges and access to the customer's underlying environment. Following such discovery, on May 30, 2023, Progress promptly (i) reached out to all MOVEit Transfer and MOVEit Cloud (Progress' cloud-hosted version of MOVEit Transfer) customers in order to apprise them of the vulnerability and alert them to immediate remedial actions, and (ii) took down MOVEit Cloud for investigation. In parallel, the engineering team at the Company worked to develop a patch for all supported versions of MOVEit Transfer (including MOVEit Cloud), which was released across all impacted systems on May 31, 2023 and allowed for the restoration of MOVEit Cloud that same day.

Form 8-K filed 6/5/2023, https://investors.progress.com/static-files/e8a76c9d-310a-4762-8853-e92a1952d6a4 (last visited Oct. 8, 2023).

8. Mandiant, a cybersecurity company and subsidiary of Google, reported that based on initial analysis from its incident response engagements, "earliest evidence of exploitation occurred on May 27, 2023 resulting in deployment of web shells and data theft. In some instances, data theft has occurred within minutes of the deployment of web shells." Nader Zaveri, et al, *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft,* Mandiant Blog, June 2, 2023, updated Aug. 16, 2023, https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft) (last visited Oct. 11 2023). Mandiant reported that "on June 6, 2023, a post on the CL0P^_-LEAKS data leak site (DLS) claimed responsibility for this activity and threatened to post stolen data if victims did not pay an extortion fee." *Id.*

9. Another cybersecurity company, Rapid7, reported that "[a]s of May 31, there were roughly 2,500 instances of MOVEit Transfer exposed to the public internet, the majority of which look to be in the United States" and that "[o]n June 6, 2023, the Cl0p gang posted a communication to their leak site demanding that victims contact them before June 14 to negotiate extortion fees for deleting stolen data." Caitlin Condon, *Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability*, Rapid7 Blog, June 1, 2023, last updated Aug. 10, 2023 https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/ (last visited Oct. 11, 2023).

10. On June 9, 2023, Progress informed its customers it "partnered with third-party cybersecurity experts to conduct further detailed code reviews as an added layer of protection" where "cybersecurity firm Huntress has helped [Progress] to uncover additional vulnerabilities that could potentially be used by a bad actor to stage an exploit" where the "newly discovered

vulnerabilities are distinct from the previously reported vulnerability shared on May 31, 2023." *MOVEit Transfer and MOVEit Cloud Vulnerability,* https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability (last visited Oct. 10, 2023).

11. On June 16, 2023, Progress wrote its customers that on the prior day it "reported the public posting of a new SQLi vulnerability that required us to take down HTTPs traffic for MOVEit Cloud and to ask MOVEit Transfer customers to take down their HTTP and HTTPs traffic to safeguard their environments." *MOVEit Transfer and MOVEit Cloud Vulnerability,* (https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability) (last visited Oct. 10, 2023). On June 18, 2023, Progress wrote that a "third party publicly disclosed a vulnerability impacting MOVEit Transfer and MOVEit Cloud in a way that did not follow normal industry standards, and in doing put our customers at increased risk of exploitation." *Id.*

12. On July 7, 2023, Progress informed its investors that "certain MOVEit Transfer customers have reported that malicious threat actors have exploited the MOVEit Vulnerability to obtain access to their environments and portions of their sensitive customer data" and that two "dedicated MOVEit Cloud customers have reported that malicious threat actors have exploited the MOVEit Vulnerability to obtain access to its environment." *Form 10-Q filed 7/7/2023,* https://investors.progress.com/static-files/90ee1d91-3191-40f0-97dd-e94d6aa26f7d (last visited Oct. 10, 2023). Third parties subsequently notified Progress of additional product vulnerabilities which Progress reportedly patched. *Id.* On October 10, 2023, Progress informed its investors that one of those MOVEit Cloud customers reported "certain personally identifiable information was exfiltrated." *10-Q filed 10/10/2023* at 33, https://investors.progress.com/static-files/7c341340-7f47-4271-ad55-3dcc6bcb2871 (last visited October 10, 2023).

13. Progress's MOVEit Transfer and MOVEit Cloud servers contained Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively, "Personal Information" of individuals, including Plaintiffs and Class members. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." S*ee Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf (last visited Oct. 11, 2023). PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq.*, as well as multiple state statutes. According to the U.S. Department of Health & Human Services ("HHS"), PHI "is information, including demographic data," that relates to: "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," or "the past, present, or future payment for the provision of health care to the individual," and that "identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual." *See Summary of the HIPAA Privacy Rule, HHS*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Oct. 11, 2023). "Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, SSN)." *Id.*

14. The Data Breach began when, according to a U.S. Cybersecurity and Infrastructure Agency ("CISA") and FBI alert, "the CL0P Ransomware Gang, also known as TA505, began exploiting a previously unknown structured query language (SQL) injection vulnerability (CVE-

2023-34362) in Progress Software's managed file transfer solution known as MOVEit Transfer beginning in May 2023. Internet-facing MOVEit Transfer web applications were infected with a specific malware used by CL0P, which was then used to steal data from underlying MOVEit Transfer databases." *See CISA and FBI Release Advisory on CL0P Ransomware Gang Exploiting MOVEit Vulnerability*, https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability (last visited Oct. 11, 2023); *see also #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability,* Cybersecurity Advisory, June 7, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a (last visited Oct. 11, 2023).

15. Emsisoft Ltd., an anti-malware and anti-virus software company tallied 2,546 organizations as impacted by the Data Breach as of October 11, 2023, including the records of approximately 64.5 million individuals, where the United States accounts for 84.1% of known impacted organizations. Zach Simas, *Unpacking the MOVEit Breach: Statistics and Analysis*, Emsisoft Blog, July 18, 2023, updated Oct. 11, 2023, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited Oct. 11, 2023). Among the organizations affected by the Data Breach with the greatest number of impacted individuals are Maximus Federal Services, Inc. ("Maximus") at 11 million individuals and Colorado Department of Health Care Policy and Financing ("HCPF") at 4 million individuals. *Id.* While Cl0p wrote in its June 6, 2023 post that data it stole from government, cities and police services had been deleted, that post was proven false when it subsequently posted data from the United Kingdom's Office of Communications ("Ofcom") and the Republic of Ireland's Commission for Communications Regulation ("ComReg.") *Id.* Emsisoft noted that some organizations were impacted through using "a vendor which used a contractor which used a

subcontractor which used MOVEit" while other organizations have had MOVEit exposure via multiple vendors." *Id.* CL0P has previously attacked file transfer platforms in similar attacks against Accellion File Transfer Appliances (FTA) in 2020 and 2021, SolarWinds Servers in 2021, and Fortrar/Linoma GoAnywhere MFT servers in 2023. *Id.* Emsisoft noted "significant potential for the stolen data to be used in spear phishing, BEC scams, etc., meaning that this one crime could act as an enabler for many other crimes." *Id.*

16. Progress's failure to reasonably secure consumers' Personal Information including PII and PHI from the foreseeable risk of its being stolen through its vulnerable MOVEit software, as exploited by CL0P, caused the Data Breach.

JURISDICATION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of Class members exceeds 100, many of whom, including Plaintiffs, have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has personal jurisdiction over this action because Defendant maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. See 28 U.S.C. § 1332(a).

19. Venue is proper in this Court under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

THE PARTIES

A. Plaintiffs

20. Plaintiffs identified below bring this action on behalf of themselves and others similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, Progress, through its actions described herein caused Plaintiffs' valuable Personal Information to be accessed and exposed by unknown and unauthorized criminals, thus causing them harm and continuing increased risk of harm.

21. Based upon counsel's investigation, and upon information and belief, residents of the State of California were injured by the Data Breach. The Plaintiff identified below is also pursing claims on behalf of citizens and residents of California.

22. Plaintiff Carin Dickmeyer is citizen and resident of the State of California. Progress obtained Plaintiff's Personal Information including PHI through Progress's customer, Maximus Federal Services, Inc. ("Maximus"). Maximus is a Centers for Medicare & Medicaid Services ("CMS") contractor that provides appeals services in support of the Medicare program.

23. Based upon counsel's investigation, and upon information and belief, residents of the State of Colorado were injured by the Data Breach. The Plaintiff identified below is also pursuing claims on behalf of citizens and residents of Colorado.

24. Plaintiff Joel Bonnett is a citizen and resident of the State of Colorado. Progress obtained Plaintiff's Personal Information including PHI through Progress's customer International Business Machine Corp. ("IBM") a vendor for the Colorado Department of Health Care Policy and Financing ("HCPF") which oversees Health First Colorado (Colorado's Medicaid program), Child Health Plan *Plus* ("CHP+"), and other health care programs for Coloradans.

B. Defendant

25. Defendant Progress Software Corporation is a Delaware corporation with its principal place of business located at 15 Wayside Road, Suite 400, Burlington, Massachusetts. Progress's common stock is publicly traded on the NASDAQ under the ticker symbol "PRGS." *Form 10-K filed 1/27/2023* (hereinafter "2022 Form 10-K") https://investors.progress.com/static-files/5c0861cf-4a3f-4f2d-b265-6c4685340c65 (last visited Oct. 11, 2023). Progress is a provider of "products to develop, deploy and manage high-impact business applications." *2022 Form 10-K* at 4. "Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals," *Progress Announces Second Quarter 2023 Financial Results*, June 29, 2023, (https://investors.progress.com/node/26296/pdf) (last visited Oct. 8, 2023), including healthcare organizations; education institutions; federal government agencies; state retirement systems; news organizations; law firms; and corporations; which obtained and maintained Plaintiffs' Personal Information that was compromised in the Data Breach. Progress has 2,071 employees worldwide. *2022 Form 10-K* at 8.

FACTUAL ALLEGATIONS

A. Progress, a Sophisticated Software Company, Collects Consumers' Personal Information, including Private Health Information

26. Progress describes itself as "the trusted provider of the best products to develop, deploy and manage high-impact business applications." *2022 Form 10-K* at 4.

27. Progress wrote that Defendant "is committed to protecting the privacy of individuals who visit [Progress's] web sites, individuals who register to use [Progress's] services, and individuals who register to attend [Progress's] corporate events." *Privacy Policy*, updated July 1, 2023, https://www.progress.com/legal/privacy-policy (last visited Oct. 8, 2023).

28. Progress advised its investors that Progress's "business practices with respect to the collection, use and management of personal information could give rise to operational interruption, liabilities or reputational harm as a result of governmental regulation, legal requirements or industry standards relating to consumer privacy and data protection." *2022 Form 10-K* at 14.

29. Progress defines two types of "Personal Information." *See* its *Supplemental Privacy Notice for Residents of California*, July 1, 2023, https://www.progress.com/legal/california-resident-privacy-notice#:~:text=The%20CCPA%2FCPRA%20allows%20you,PIN%20689%20150%20when%20prompted (last visited Oct. 10, 2023). Progress defines "**Personal Information**" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with you or your household such as your real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, other similar identifiers." Progress defines "**Sensitive Personal Information**" as "Social Security number (SSN), driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account," while excluding "publicly-available information, deidentified or aggregated consumer information and certain other information that is regulated by other applicable laws." *See id.*

30. Progress notified California residents that it collects the following categories of personal information:

- **Identifiers** (e.g. real name, address, social security number)
- Characteristics of protected classification under California or Federal law;
- **Commercial information** (e.g. products purchased, obtained, or considered, or other purchasing or consuming histories)

- **Internet or other electronic network activity** (e.g. browsing history, search history, or a consumer's interaction with a website)
- Geolocation data
- Audio, visual, and similar information
- Professional or employment related information
- **Education information** (information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act)
- **Inferences drawn from any of the information above to create a profile about a consumer** (reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and attitudes)
- **Account log-in**, password, or credentials allowing access to an account.

Id.

31. Progress notified California residents that it obtains Personal Information from consumers from the following categories of sources:

- Directly from you. For example, from forms you complete or products and services you purchase from [Progress].
- Indirectly from you. For example, from observing and/or tracking your browsing activity on [Progress's] websites.
- From [Progress's] Partners. For example, when they register your contact information with [Progress] as a lead or an end user.
- From third-party marketing companies who provide [Progress] with sales leads.
- Through your interactions with [Progress] on social media (e.g., Facebook, LinkedIn, Twitter, Instagram, etc.)
- From events or webinars organized or sponsored by [Progress].

Id.

32. As a sophisticated software company selling software products and solutions healthcare companies, Progress knew it subjected itself to Health Insurance Portability and

Accountability Act of 1996 ("HIPAA") and Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") requirements to comply with provisions designed to protect the privacy of patients' valuable Personal Information including Protected Health Information ("PHI") which, according to Progress's *HIPAA Compliance FAQs*, includes "any information about health status, health care treatment, or healthcare payment that is created by a Covered Entity or Business Associate and can be linked to a specific individual," where Progress described HIPAA Covered Entities as "institutions, organizations, or individuals who electronically transmit any health information in connection with transactions for which HIPAA has adopted standards" including "(1) health plans, (2) health care clearinghouses, and (3) health care providers," and described a "Business Associate" as a person or entity that performs certain functions on behalf of a Covered Entity that involve the use or disclosure of protected health information," and where Progress provides HIPAA covered entities with a "Business Associate Agreement." https://www.progress.com/legal/hipaa-compliance-faqs (last visited Oct. 10, 2023).

33. Consumers' Personal Information, including PII and PHI was collected by Progress which failed to prevent the Personal Information from being accessed and exposed by CL0P, an unauthorized third party, in the Data Breach.

B. Progress Shares Consumers' Personal Information with Advertisers, Payment Processors and Other Service Providers

34. Progress advised its investors that:

> [G]overnmental entities in the U.S. and other countries have enacted or are considering enacting legislation or regulations, or may in the near future interpret existing legislation or regulations, in a manner that could significantly impact [Progress's] ability and the ability of [Progress's] customers and data partners to collect, augment, analyze, use, transfer and share personal and other information that is integral to certain services

> [Progress] provide[s]. For example, the California Privacy Rights Act (which amends the California Consumer Privacy Act) took effect on January 1, 2023; Virginia, Colorado, Utah and Connecticut also have privacy laws taking effect in 2023….

2022 10-K at 14.

35. Progress disclosed to California residents that it sells consumers' personal information where "'selling' is broadly defined as 'selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.'" *Supplemental Privacy Notice for Residents of California*, effective July 1, 2023, updated June 20, 2023, https://www.progress.com/legal/california-resident-privacy-notice (last visited Oct. 8, 2023).

36. Progress disclosed to California residents it may "share, disclose [consumers'] personal information to a third party for a business purpose or 'sell' or share [consumers'] personal information," where third parties include Progress's "Service Providers;" "Partners;" Progress's "subsidiaries and affiliates;" Internet cookie data recipients, data analytics providers, and social media networks; and "Industry Analysts." *Id.*

37. Progress's Partners include the following partner types: (i) Distributor; (ii) Value Added Reseller; (iii) Service Delivery Partner; (iv) Digital Agency; (v) Managed Service Provider; (vi) Systems Integrator; (vii) Independent Software Vendor; (viii) Technology Alliance Partner. *See Progress Partners Network,* https://www.progress.com/partners (last visited Oct. 10, 2023).

38. Progress advised its investors its "products are generally sold as perpetual licenses, but certain products also use term licensing models and [Progress's] cloud-based offerings use a subscription-based model. More than half of [Progress's] worldwide license revenue is realized

through relationships with indirect channel partners….” Progress “operate[s] in North America, Latin America, Europe, the Middle East and Africa (‘EMEA’), and Asia and Australia (‘Asia Pacific’), through local subsidiaries as well as independent distributors.” *2022 10-K* at 43.

39. Progress shares and sells consumers’ Personal Information including PII and PHI with third parties for profit and that Personal Information was accessed and exposed by CL0P, an unauthorized third party during the Data Breach.

C. Progress Knew of the Risk that Cybercriminals Posed to Consumers’ Personal Information and Private Health Information

40. Progress advised its investors on the following risk:

> *If [Progress’s] security measures are breached, [Progress’s] products and services may be perceived as not being secure, customers may curtail or stop using [Progress’s] products and services, and [Progress] may incur significant legal and financial exposure. including but not limited to from loss of customer or company data, loss of customers or otherwise.*

2022 10-K at 13.

41. Progress reported its “business practices with respect to the collection, use and management of personal information could give rise to operational interruption, liabilities or reputational harm as a result of governmental regulation, legal requirements or industry standards relating to consumer privacy and data protection.” *Id.* at 14.

42. Progress advised investors it was “subject to varied and complex laws, regulations and customs, both domestically and internationally” relating to “a number of aspects of [Progress’s] business, including … data and transaction processing security, payment card industry data security standards, records management, user-generated content hosted on websites we operate, data privacy or related privacy practices, data residency, corporate governance.”

Id. Progress continued:

> Compliance with these laws and regulations may involve significant costs or require changes in [Progress's] business practices that result in reduced revenue and profitability. Non-compliance could also result in fines, damages, criminal sanctions against [Progress] …, prohibitions on the conduct of [Progress's] business, and damage to [Progress's] reputation.

Id.

43. Despite knowing of the risk that cybercriminals posed to consumers' Personal Information including PII and PHI, Progress failed to deploy adequate cybersecurity measures to prevent CL0P, a Russian cybercriminal gang from gaining unauthorized access to consumers' Personal Information and exposing it during the Data Breach.

D. Progress had a Responsibility to Safeguard Consumer's Personal Information and Private Health Information

44. Progress informed its investors:

> Any security breach or unauthorized access could result in significant legal and financial exposure, increased costs to defend litigation, indemnity and other contractual obligations, government fines and penalties, damage to our reputation and our brand, and a loss of confidence in the security of our products and services that could potentially have an adverse effect on our business and results of operations. Breaches of our network could disrupt our internal systems and business applications, including services provided to our customers.

Id. at 12.

45. Progress advised its investors that:

> [Progress] may need to spend significant capital or allocate significant resources to ensure effective ongoing protection against the threat of security breaches or to address security related concerns. If an actual or perceived breach of [Progress's] security occurs, the market perception of the effectiveness of [Progress's] security measures could be harmed and [Progress] could lose customers. In addition, [Progress's] insurance coverage may not be adequate to cover all costs related to cybersecurity incidents and the disruptions resulting from such events.

Id. at 13.

46. Progress further advised investors that if its products contain security flaws it could harm Progress's revenue and expose Progress to litigation. *Id.* at 13. Progress advised its software products "may contain defects or security flaws" and Progress "may need to issue corrective releases of [its] software products to fix any defects or errors." *2022 Form 10-K* at 13. "Depending upon the severity of any such events, the detection and correction of any security flaws can be time consuming and costly," and errors in the software products could "adversely affect market acceptance" and expose Progress to potential litigation. *Id.* at 13.

47. Progress wrote that businesses must comply with numerous regulations where "[n]on-compliance can result in severe consequences, including financial penalties, loss of customer and investor confidence, and even prosecution," noting that businesses that do not comply with the European Union's General Data Protection Regulation of 2016 ("GDPR") can be fined up to 20 million euros or 4% of global revenue, noted the "U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA)," "regulates the handling of protected health information (PHI)," the "Federal Trade Commission (FTC)" "regulates advertising, marketing, and consumer protection," and the Payment Card Industry Data Security Standard (PCI DSS)" "regulates the

handling of credit card information." John Iwuozor, *The Role of Business Rules in Regulatory Compliance: How Progress Corticon.js Can Help*, Progress, July 18, 2023, https://www.progress.com/blogs/role-business-rules-regulatory-compliance-how-progress-corticon-js-can-help (last visited Oct. 11, 2023).

48. Progress wrote "[a]lthough HIPAA primarily applies to medical providers and insurance companies that deal in patient data on a regular basis, business associates are impacted by this law as well. So even if you're not building a website, app or patient portal for, say, a hospital, physician's office or health insurance carrier, organizations that partner with medical entities such as these can be subject to HIPAA's regulations." Suzanne Scacca, *The High Stakes of Regulatory Compliance and Digital Products*, Progress, https://www.progress.com/blogs/high-stakes-regulatory-compliance-digital-products (last visited Oct. 11, 2023) (internal hyperlink omitted). Progress is such a Business Associate subject to HIPAA's regulations.

49. As a Business Associate of HIPAA Covered Entities, Progress knew it was required to safeguard PHI according to Progress's *HIPAA Compliance FAQs*, where under HIPAA's Privacy Rule, Business Associates such as Progress must "implement appropriate safeguards to protect the privacy of PHI," and where Progress must notify Covered Entities of a breach of PHI. https://www.progress.com/legal/hipaa-compliance-faqs (last visited Oct. 10, 2023).

50. Progress advised in its *HIPAA Compliance FAQs*, that to comply with HIPAA Progress:

> [O]perates secure computing environments in its corporate offices, development environments, and production cloud products. Each of these areas are equipped with security technologies, processes, and people needed to protect sensitive information. The Progress Internal Audit team audits use of security solutions and

> processes, evaluated by annual SOC2 assessments and validated by annual HIPAA audits. Copies of the SOC2 assessments and audit reports are available to our customers upon request. Progress corporate administration and human resources functions are also audited for HIPAA compliance on an annual basis.

Id.

51. Progress attempted to differentiate itself from its competitors by answering *HIPAA Compliance FAQs* question, "What is unique about Progress' security practices?" by writing:

> Security is part of everyone's responsibility at Progress. From development to production, employees across all areas of the company are charged with incorporating security into their duties. Whether it is physical security of their work areas, secure coding during the development process, network security, cloud security, or participating in audits, keeping our environment and our products safe is part of everyone's job.

https://www.progress.com/legal/hipaa-compliance-faqs (last visited Oct. 10, 2023).

52. Progress also advised, "Health data protection don't end with HIPAA. The FTC has put something in place called the Health Breach Notification Rule. This rule impacts anyone not covered by HIPAA. So if your product handles personal health information that doesn't identify who the patient is, then you'd be subject to this one." Suzanne Scacca, *The High Stakes of Regulatory Compliance and Digital Products,* Progress, https://www.progress.com/blogs/high-stakes-regulatory-compliance-digital-products (last visited Oct. 11, 2023).

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential

consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

54. Progress also advises that since 2004, the Payment Card Industry Dat Security Standard (PCI DSS) "refers to a list of 12 security standards related to the processing of credit cards and credit card data" and that failure to comply can result in heavy fines, and that if a website gets hacked, a "company will be on the line for the data breach and monetary loss" so "implementing the security standards above is critical." According to Progress, the FTC's "Safeguards Rule" "aims to protect private personal information that financial institutions collect from customers" so companies "building digital products" for such institutions must be mindful of the regulations. Suzanne Scacca, *The High Stakes of Regulatory Compliance and Digital Products*, Progress, https://www.progress.com/blogs/high-stakes-regulatory-compliance-digital-products, (last visited Oct. 11, 2023). Financial institutions are among Progress's MOVEit customers.

55. Progress knows that while GDPR protects EU citizens, "anyone collecting data on them is accountable to this law. This applies to everyone—from California-based ecommerce websites selling goods to bloggers in Melbourne who have newsletter subscription forms on their sites." *Id.* Progress is subject to the GDPR's regulations.

56. Progress purports to operate an Information Security Program and supporting policy framework "to protect the security interests of company infrastructure, the software it produces, and customer solutions it operates" and which is "responsible for protecting the confidentiality, integrity, and availability of information handled by company technology systems and outwardly facing technology products" in order to "identify, assess, monitor, and remediate

security issues in a manner that keeps risks under control and within company and customer appetite" in accordance with "applicable laws, regulations, and industry best practices." *Information Security Program Whitepaper*, Progress, https://www.progress.com/security/information-security-program-whitepaper (last visited Oct. 11, 2023).

57. Progress advises that it "conducts a range of compliance activities throughout the course of any given year" focusing on "Sarbanes-Oxley (SOX), SOC2, HIPAA, and GDPR" compliance and assures that its "engineers work together within products and across products to ensure best practices in security design are implemented and maintained." *Id.*

58. The *Progress Software Corporation Data Processing Addendum*, or "DPA" is intended to "ensure adequate safeguards with respect to the privacy and security of Personal Data passed from Customer to Progress for Processing on the Customer's behalf, as authorized by customer" is "an addendum to each end user license agreement, master agreement, professional services agreement or other agreement between Customer and Progress pertaining to the licensing of products and/or the delivery of Services by Progress…." https://www.progress.com/docs/default-source/progress-software/data-processing-addendum.pdf (last accessed Oct. 11, 2023). Progress agreed to "maintain appropriate technical and organizational security measures for the Processing of Personal Data" to protect "Personal Data against … unauthorized loss, destruction, disclosure or access…." *Id.* at 5.

59. Progress's *Privacy Center* highlights that it purportedly "implemented technical and organizational measures to ensure HIPAA compliance," that it "implemented measures to address the requirements of the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights act and its regulations," and assures "Progress is Committed to

Protecting Your Personal Information." https://www.progress.com/legal/privacy-center (last visited Oct. 11, 2023).

60. Progress CEO Yogesh Gupta discussed the Data Breach with Progress's investors on June 29, 2023, and stated that Progress's "focus throughout this process has been on supporting [its] customers in securing their environment" and "doing what [it] can to protect [its] customers against the ongoing threat of cybercriminals." *Progress Software Corporation (NASDAQ: PRGS) Q2 2023 Earnings Call Transcript* at 4, Insider Monkey Transcripts, July 2, 2023, https://www.insidermonkey.com/blog/progress-software-corporation-nasdaqprgs-q2-2023-earnings-call-transcript-1164155/?singlepage=1 (Oct. 8, 2023).

61. Despite its responsibilities, duties, commitments, representations, and assurances, Progress failed to adequately safeguard, secure and protect Plaintiffs' consumers' Personal Information collected from its clients, allowing that Personal Information to be accessed and exposed by an unauthorized third party, CL0P.

E. Progress Knew it was a Target for Cybersecurity Attacks and Data Breaches and was Vulnerable to Such Attacks

62. Progress advised its investors of the risk that if Progress's "security measures are breached," its "products and services may be perceived as not being secure" and customers may stop using Progress's products and Progress "may incur significant legal and financial exposure" including from "lost of customer or company data…." *2022 Form 10-K* at 12:

63. Progress already had a recent data breach prior to the Data Breach at hand, it reported to its investors and the SEC regarding the previous exploitation of vulnerabilities in Progress's cybersecurity program:

> As disclosed on December 19, 2022, following the detection of irregular activity on certain portions of our corporate network, we engaged outside cybersecurity

> experts and other incident response professionals to conduct a forensic investigation and assess the extent and scope of the cyber incident. During the investigation, we and our external advisors uncovered evidence of unauthorized access to our corporate network, including evidence that certain company data had been exfiltrated.

See 2022 Form 10-K at 12; *see Form 8-K filed 12/19/2022*, https://investors.progress.com/static-files/b1f73d79-c30d-4044-ac0a-7f0f2963f8cb (last visited Oct. 10, 2023).

64. Progress further advised its investors:

> As demonstrated by [the] cyber incident [Progress disclosed on December 19, 2022], due to the actions of outside parties, employee error, malfeasance, or otherwise, an unauthorized party may obtain access to our data or our customers' data, which could result in its theft, destruction, corruption or misappropriation and thus legal and financial exposure. Security risks in recent years have increased significantly given the increased sophistication and activities of hackers, organized crime, including state-sponsored organizations and nation-states, and other outside parties.

2022 Form 10-K at 12.

65. Progress reported, "Cyber threats are continuously evolving, increasing the difficulty of defending against them. Increased risks of such attacks and disruptions also exist due to the Russian invasion of Ukraine beginning in February 2022. *Id.* The harm of the risk of Russian based cybersecurity attacks was realized in the Data Breach. See Zach Montague, *Russian Ransomware Group Breached Federal Agencies in Cyberattack*, The New York Times, June 15, 2023, https://www.nytimes.com/2023/06/15/us/politics/russian-ransomware-cyberattack-clop-

moveit.html (last visited Oct. 11, 2023). According to Jen Easterly, director of the CyberSecurity and Infrastructure Security Agency ("CISA"), CL0P is a Russian ransomware gang. *Id.*

66. Progress maintains $15 million of cybersecurity insurance coverage which it expects to reduce Progress's exposure to cybersecurity incidents and data breaches. *See Form 10-Q filed 10/10/2023,* at 34. https://investors.progress.com/static-files/7c341340-7f47-4271-ad55-3dcc6bcb2871 (last visited Oct. 10, 2023).

67. Despite Progress's knowledge that it was a target for cybersecurity attacks and the heightened risk that consumers' Personal Information it collected from its customers could be accessed and exposed by unauthorized third parties such as CL0P given the known vulnerabilities of Progress's cybersecurity program, Progress failed to adequately protect that Personal Information.

F. Progress Ignored Government and Industry Guidance, Standards, and Best Practices for Preventing Cybersecurity Attacks and Data Breaches, Causing the Data Breach to Occur

68. Federal and state governments have established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making. *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdffi205-startwithsecurity.pdf (last visited Oct. 11, 2023).

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business. FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Oct. 11, 2023). The

guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. *Id.* The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

70. Progress informed its investors that Progress is facing "several inquiries from domestic and foreign data privacy regulators" as well as "several state attorneys general." *Form 10-Q filed 10/10/23* at 34, https://investors.progress.com/static-files/7c341340-7f47-4271-ad55-3dcc6bcb2871 (last visited Oct. 10, 2023). Progress is also facing "formal investigations" from "a U.S. federal law enforcement agency" and the SEC. *Id.* Progress received a subpoena from the SEC on October 2, 2023 regarding the Data Breach. *Id.*

71. Despite its duties, representations, and assurances, Progress failed to adequately secure and protect its clients' data including consumers' Personal Information, allowing that Personal Information to be accessed and exposed by an unauthorized third party, CL0P.

G. Progress Ignored its Own Information Security Policies, Causing the Data Breach to Occur

72. Progress advises that it:

> [O]perates an Executive Security Committee which has directed that a security program and supporting policy framework be operated to protect the security interests of company infrastructure, the software it produces, and customer solutions it operates. The company information security program is responsible for protecting the confidentiality, integrity, and availability of information handled by

> company technology systems and outwardly facing technology products. It is established that this function will identify, assess, monitor, and remediate security issues in a manner that keeps risks under control and within company and customer appetite.

Information Security Whitepaper, Progress, https://www.progress.com/security/information-security-program-whitepape (last visited Oct. 11, 2023). Progress assured that the program "is operated according to applicable laws, regulations, and industry best practices." *Id.* Progress advises that it "conducts a range of compliance activities throughout the course of any given year" which focus on "Sarbanes-Oxley (SOX), SOC2, HIPAA, and GPR." *Id.*

73. With respect to "GDPR Related Controls," Progress advises "All systems and applications are protected by a defense in depth security strategy that features robust physical security, firewall, access control, antivirus, encryption, monitoring, and other defenses. These controls are examined routinely as part of company HIPAA, SOC2, and SOX programs." *Id.* Progress wrote "Technical or organizational measures to ensure that personal data are not read, copied, altered or removed during processing or without authorization. Production systems are highly secured and monitored for anomaly behavior. Corporate networks are equipped with intrusion detection systems capable of identifying attempted exfiltration." *Id.* If Progress employed such measures, CL0P would not have been able to exfiltrate large amounts of Personal Information during the Data Breach.

74. Regarding "Product Security," Progress wrote:

> All software products at progress are developed avia the use of modern methodologies, techniques, technologies, and processes. [Progress's] software development life cycles employ Agile methodologies while including numerous waves of security planning and

> testing. These include security requirements planning, security design planning, code level security scanning, vulnerability scanning, and penetration testing.

Id. If Progress employed a secure software development lifecycle, its MOVEit Transfer and MOVEit Cloud products would not have been vulnerable to exploitation by CL0P during the Data Breach.

H. Progress's Failure to Follow Government and Industry Standards and its Own Information Security Policy Resulted in a Data Breach where CL0P, an Unauthorized Party, Accessed and Exposed Plaintiffs' and Class Members' Personal Information

75. Progress advised its investors:

> We are subject to risks associated with compliance with laws and regulations globally, which may harm our business. We are a global company subject to varied and complex laws, regulations and customs, both domestically and internationally. These laws and regulations relate to a number of aspects of our business, including trade protection, import and export control, data and transaction processing security, payment card industry data security standards, records management, user-generated content hosted on websites we operate, data privacy or related privacy practices, data residency, corporate governance, anti-trust and competition, employee and third-party complaints, anti-corruption, gift policies, conflicts of interest, securities regulations and other regulatory requirements affecting trade and investment.

2022 Form 10-K at 14.

76. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

77. For example, in 2019, both Microsoft and Google have publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!" Matt Bromiley, *Bye Passwords: New Ways to Authenticate at 3*, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ (last visited Oct. 11, 2023). An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

78. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks." *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/blog/what-is-multi-factor-authentication/ (last visited Oct. 11, 2023).

I. Plaintiffs' and Class Members' Personal Information including PHI are Valuable

79. Personal Information Its value is axiomatic, considering the market value and profitability of" Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2022 Annual Report a total annual revenue of $282.8 billion and net income of $60 billion. *Alphabet Inc. Form 10-K filed 2/3/2023* at 30, https://www.sec.gov/Archives/edgar/data/1652044/000165204423000016/goog-20221231.htm (last visited Oct. 11, 2023). $253.5 billion of that revenue derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about the users of its various free products and services. America's largest corporations profit almost exclusively

through the use of Private Information illustrating the considerable market value of personal Private Information. *Id.* at 32.

80. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

81. Cybercriminals use "ransomware" to make money and harm victims. Ransomware is a widely known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

82. Stolen Personal Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a TOR browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

83. The FBI's Internet Crime Complaint Center ("IC3") reported that in "2022, the IC3 received 800,944 complaints" regarding cyberattacks and cyber-enabled frauds representing more

than $10.2 billion in total potential loss. *2022 IC3 Report*, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf at 3. "In 2022, the IC3 received 2,385 complaints identified as ransomware with adjusted losses of more than $34.3 million." *Id.* at 13. "In 2022, the IC3 has seen an increase in an additional extortion tactic used to facilitate ransomware. The threat actors pressure victims to pay by threatening to publish the stolen data if they do not pay the ransom." *Id.*

84. According to HHS and the "Healthcare & Public Health Sector Council," "[h]ealthcare records continue to be one of the most lucrative items on the underground market, ranging from $250 to $1,000 compared to other items like credit cards only selling for an average $100. This demonstrates the value of data like Protected Health Information (PHI) to cyber-attackers and their motivation for attacking healthcare institutions. Therefore, protecting a patient's health information and PHI is paramount at every level of an organization, from practitioners to executives."

85. The United States Department of State, Rewards for Justice Program posted a $10 million reward on "X," the company formerly known as Twitter, for information related to the CL0P ransomware gang and created a dedicated TOR link to receive tips. @RFJ_USA, July 26, 2023, https://twitter.com/RFJ_USA/status/1669740545403437056 (last visited Oct. 12, 2023).

86. Cybersecurity blog BleepingComputer reported that the CL0P "ransomware gang is expected to earn between $75-100 million from extorting victims of their massive MOVEit data theft campaign." Lawrence Abrams, *Clop gang to earn over $75 million from MOVEit extortion attacks,* BleepingComputer, https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/ (last visited Oct. 12, 2023).

87. As a sophisticated software company engaged in the collection, distribution, sharing, and sale of consumers' Personal Information, Progress knew it subjected itself to FTC requirements to comply with provisions designed to protect the privacy of consumer's Personal Information.

88. Progress knew or should have known that consumer's Personal Information, including PII and PHI is valuable, and therefore a prime target for criminals. Progress should have taken adequate steps to protect that Personal Information from Data Breaches.

89. Progress failed to take reasonable and adequate steps to prevent patients' Personal Information from being accessed by an unauthorized party and exposed in the Data Breach.

J. Plaintiffs' Experiences

1. ***California***

90. Plaintiff Carin Dickmeyer is a resident and citizen of California. Plaintiff Dickmeyer is acting on her own behalf and on behalf of those similarly situated. Progress obtained and continues to maintain Plaintiff Dickmeyer's Personal Information and has a legal duty and obligation to protect that Personal Information from unauthorized access and disclosure.

91. Progress has a further duty to provide Plaintiff Dickmeyer with prompt and accurate notice when her Personal Information has been accessed and disclosed by unauthorized parties in a data breach on Progress's servers.

92. Plaintiff Dickmeyer would not have entrusted her Personal Information to one or more of Progress's customers had she known that one of the customer's information technology vendors entrusted with her Personal Information failed to maintain adequate data security.

93. Plaintiff Dickmeyer's Personal Information was accessed by an unauthorized party, CL0P, and disclosed as a result of the Data Breach.

94. On or around July 28, 2023, Plaintiff Dickmeyer received a letter from Maximus Federal Services, Inc. ("Maximus") informing her that "an incident involving [her] personal information related to services provided by Maximus." *See July 28, 2023 Maximus Letter to Carin Dickmeyer*, **Exhibit A**.

95. Maximus is a "CMS contractor that provides appeals services in support of the Medicare program. *See Id.* Maximus informed Dickmeyer that the "incident involved a security vulnerability in the MOVEit software, a third-party application which allows for the transfer of files during the Medicare appeals process." *See id.*

96. Maximus notified Plaintiff Dickmeyer that if her Medicare Beneficiary Identifier ("MBI") was "impacted," she would receive "a new Medicare card with a new Medicare Number." *See id.*

97. Maximus notified Plaintiff Dickmeyer that on "May 30, 2023, Maximus detected unusual activity in its MOVEit application." *Id.* On May 31, 2023 Maximus began to investigate and stopped all use of the MOVEit application. *Id.* Later that day, "Progress Software Corporation, announced that a vulnerability in its MOVEit software had allowed an unauthorized party to gain access to files across may organizations in both the government and private sectors." *Id.*

98. Maximus informed Plaintiff Dickmeyer that it notified CMS of the Data Breach on June 2, 2023. *Id.* Maximus wrote that the "ongoing investigation indicates that on approximately May 27 through 31, 2023, the unauthorized party obtained copies of files that were saved in the Maximus MOVEit application, but that no CMS system has been compromised." *Id.* Maximus analyzed those files and "determined that those files contained some of [Plaintiff's] personal information." *Id.*

99. Maximus wrote Plaintiff Dickmeyer that it determined her "personal and Medicare information was involved" in the Data Breach and may have included her name; Social Security Number or Individual Taxpayer Identification Number; Date of Birth; Mailing Address; Telephone Number, Fax Number, & Email Address; Medicare Beneficiary Number (MBI) or Health Insurance Claim Number (HICN); Driver's License Number and State Identification Number; Medical History/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.); Healthcare Provider and Prescription Information; Health Insurance Claims and Policy Subscriber Information; and health Benefits and Enrollment Information. *Id.*

100. On July 26, 2023 Maximus filed an 8-K report with the SEC, informing its investors:

> On May 31, 2023, Progress Software Corporation, the developer of MOVEit ("MOVEit"), a file transfer application used by many organizations to transfer data, announced a critical zero-day vulnerability in the application that allowed unauthorized third parties to access its customers' MOVEit environments. It appears that a significant number of commercial and government customers worldwide were affected by this vulnerability. Maximus, Inc. ("Maximus" or the "Company") uses MOVEit for internal and external file sharing purposes, including to share data with government customers pertaining to individuals who participate in various government programs. The Company believes that the personal information of a significant number of individuals was accessed by an unauthorized third party by exploiting this MOVEit vulnerability.

8-K filed July 26, 2023

https://www.sec.gov/Archives/edgar/data/1032220/000103222023000061/mms-20230726.htm (last visited Oct. 12, 2023). Maximus reported it "believes those files contain personal information, including social security numbers, protected health information and/or other personal information, of at least 8 to 11 million individuals to whom the Company anticipates providing notice of the incident." *Id.*

101. In its July 28, 2023 Press Release, CMS notified "Potentially Involved Beneficiaries" that a "May 2023 data Breach in Progress Software's MOVEit Transfer software on the corporate network of Maximus Federal Services, Inc." "involved Medicare beneficiaries' personally identifiable information (PII) and/or protected health information (PHI)." CMS Responding to Data Breach at Contractor, CMS, https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor (last visited Oct. 12, 2023). CMS estimated "the MOVEit breach impacted approximately 612,000 current Medicare beneficiaries." *Id.*

102. Plaintiff Dickmeyer provided her Personal Information including PII and PHI to the U.S. Centers for Medicare & Medicaid Services ("CMS") in order to obtain Medicare benefits and services and therefore indirectly provided her information to Maximus and to Progress. Plaintiff Dickmeyer would not have entrusted her Personal Information to Progress if she did not believe that Progress would adequately safeguard her Personal Information and notify her in the event her Personal Information was accessed and exposed by an unauthorized third party, such as CL0P, in a data breach.

103. As a result of Progress's Data Breach, Plaintiff Dickmeyer was harmed by receiving a significant increase in spam and phishing emails and must expend time to review the emails and determine if the emails are legitimate.

104. Progress's Data Breach has caused Plaintiff Dickmeyer to experience increased anxiety and to suffer emotional distress due to Plaintiff's loss of privacy and due to increased risk of criminals exploiting Plaintiff's Personal Information to commit additional crimes including fraud and identity theft against Plaintiff. Criminals perpetrate fraud and identity theft through such means as sending a great number of illegitimate phishing emails which are often designed to access consumers' systems and steal consumers' financial information.

105. Plaintiff Dickmeyer has also suffered emotional distress given Plaintiffs' increased risk of further harm given the exposure of Plaintiff's Personal Information resulting from Defendant's failure to adequately secure and protect Plaintiff's Personal Information. Criminals steal Personal Information to perpetrate further crimes including identity theft and fraud. Progress's exposure of Plaintiffs' Personal Information directly harmed Plaintiff by greatly increasing the risk of Plaintiff becoming a victim of identity theft or fraud.

106. Progress also harmed Plaintiff Dickmeyer through causing Plaintiff to spend time mitigating the additional imminent harm that is at a greatly increased risk of occurring through the actions of criminals who were able to access Plaintiff's exposed Personal Information as a direct and proximate result of Progress's Data Breach.

107. Plaintiff Dickmeyer's Personal Information would not have been accessed and exposed by an unauthorized third party, i.e., CL0P, if Progress had fulfilled its responsibility to safeguard her Personal Information including PII and PHI through adequate security practices.

2. ***Colorado***

108. Plaintiff Joel Bonnett is a resident and citizen of Colorado. Plaintiff Bonnett is acting on his own behalf and on behalf of those similarly situated. Progress obtained and continues to maintain Plaintiff Bonnett's Personal Information and has a legal duty and obligation to protect that Personal Information from unauthorized access and disclosure.

109. Progress has a further duty to provide Plaintiff Bonnett with prompt and accurate notice when his Personal Information has been accessed and disclosed by unauthorized parties in a data breach on Progress's servers.

110. Plaintiff Bonnett would not have entrusted his Personal Information to one or more of Progress's customers had he known that one of the customer's information technology vendors entrusted with his Personal Information failed to maintain adequate data security.

111. Plaintiff Bonnett's Personal Information was accessed by an unauthorized party, CL0P, and disclosed as a result of the Data Breach.

112. Plaintiff Bonnett provided his Personal Information including PII and PHI to the Colorado Department of Health Care Policy & Financing ("HCPF") in order to obtain healthcare services and benefits.

113. On or about August 11, 2023, Plaintiff Bonnett received a letter from HCPF regarding a "recent incident" that involved his "personal information and/or protected health information." *August 11, 2023 HCPF Letter*, **Exhibit B**. HCPF wrote it oversees health care programs for Coloradans including Health First Colorado and Child Health Plan Plus (CHP+), and that on:

> May 31, 2023, Progress Software discovered a problem affecting its MOVEit® Transfer application. IBM, a third-party vendor contracted with HCPF, uses the MOVEit application to move HCPF data files in the normal course of business. Progress Software publicly announcer that the MOVEit problem was the result of a cybersecurity incident, which impacted may users around the world, including IBM.

Id. IBM notified HCPF that it was "impacted by the MOVEit incident" and HCPF investigated, determining on June 13, 2023 that "certain HCPF files on the MOVEit application used by IBM were accessed by the unauthorized actor on or about May 28, 2023" and the files contained Health First Colorado and CHP+ members' information, including information belonging to Plaintiff Bonnett. *Id.*

114. HCPF informed Plaintiff Bonnett that it was required by Colorado state law and HIPAA to provide Bonnett notice of the Data Breach. *Id.* HCPF wrote the information may have included Plaintiff Bonnett's full name, Social Security number, Medicaid ID number, Medicare ID number, date of birth, home address and other contact information, demographic or income information, clinical and medical information (such as diagnosis/condition, lab results, medication, or other treatment information), and health insurance information. *Id.*

115. HCPF reported to the Office of the Maine Attorney General that over 4 million (4,187,732) individuals were affected by the Data Breach. Data Breach Notifications, Colorado Department of Health Care Policy and Financing, https://apps.web.maine.gov/online/aeviewer/ME/40/804cfdd6-55c5-4775-b0ed-d21a2333ad41.shtml (last visited Oct 12, 2023).

116. Plaintiff Bonnett provided his Personal Information including PII and PHI to HCPF in order to obtain healthcare services and benefits and therefore indirectly provided his information to IBM and to Progress. Plaintiff Bonnett would not have entrusted his Personal Information to Progress if he did not believe that Progress would adequately safeguard his Personal Information and notify him in the event her Personal Information was accessed and exposed by an unauthorized third party, such as CL0P, in a data breach.

117. Progress harmed Plaintiff Bonnet through causing Plaintiff to spend time mitigating the additional imminent harm that is at a greatly increased risk of occurring through the actions of criminals who were able to access Plaintiff's exposed Personal Information as a direct and proximate result of Progress's Data Breach.

118. As a result of Progress's Data Breach, Plaintiff Bonnett was harmed by having had to expend money and time obtaining credit monitoring and identity protection services when he was unable to access the services offered by HCPF.

119. Plaintiff Bonnett has spent time checking whether his various personal accounts have been stolen and plans to change his bank account information.

120. Plaintiff Bonnett's Personal Information would not have been accessed and exposed by an unauthorized third party, *i.e.*, CL0P, if Progress had fulfilled its responsibility to safeguard his Personal Information including PII and PHI through adequate security practices.

CLASS ACTION ALLEGATIONS

121. Plaintiffs bring this lawsuit as a prospective class action on behalf of themselves and all others similarly situated as members of the proposed Classes pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), (b)(3) and (c)(4). As described below, this action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rules 23(a) and 23(b)(3). This action also satisfies the requirements of Rules 23(b)(2) and (c)(4).

122. Pursuant to Fed. R. Civ. Proc. 23(a) and (b)(2), (b)(3) and/or (c)(4), Plaintiffs assert classes based on the applicable state law of the plaintiffs. The Class and Subclasses are defined as:

123. **Nationwide Class:** All individuals residing in the United States whose Personal Information including Personally Identifiable Information and/or Protected Health Information was accessed by an unknown and unauthorized party and exposed as a result of the Data Breach.

124. **California Subclass**: All those who residing in the State of California whose Personal Information including Personally Identifiable Information and/or Protected Health Information was accessed by an unknown and unauthorized party and exposed as a result of the Data Breach.

125. **Colorado Subclass**: All those who residing in the State of Colorado whose Personal Information including Personally Identifiable Information and/or Protected Health Information was accessed by an unknown and unauthorized party and exposed as a result of the Data Breach.

126. Excluded from the Class and California Subclass and Colorado Subclass (the "Subclasses") are (1) Defendant, any entity or division in which Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; (3) any Judge sitting in the presiding state and/or federal court system who may hear an appeal of any judgment entered; and (4) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiffs reserve the right to amend the Class and Subclass definitions if discovery and further investigation reveal that the Class or any Subclass should be expanded or otherwise modified.

127. **Numerosity under Federal Rule of Civil Procedure 23(a)(l)**. Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, upon information and belief, this Class consists of millions of individuals whose Personal Information was accessed and exposed in the Data Breach, a number great enough such that joinder is impracticable. The Class members are readily identifiable from information and records in Progress's custody and control.

128. **Commonality under Federal Rule of Civil Procedure 23(a)(2)**. There are questions of law and fact common to Plaintiffs and Class members, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Progress unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Personal Information;

b. Whether Progress failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information accessed by CL0P, and unauthorized party, and exposed in the Data Breach;

c. Whether Progress truthfully represented the nature of its security systems, including their vulnerability to cybercriminals;

d. Whether Progress's data security programs prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA and the FTCA;

e. Whether Progress's data security programs prior to and during the Data Breach were consistent with industry standards;

f. Whether Progress owed a duty to Class members to safeguard their Personal Information;

g. Whether Progress breached its duty to Class members to safeguard their Personal Information;

h. Whether cybercriminals, *e.g.,* CL0P, obtained, sold, copied, stored or released Class members' Personal Information;

i. Whether Progress knew or should have known that its data security programs and monitoring processes were deficient;

j. Whether Class members suffered legally cognizable damages as a result of Progress's misconduct;

k. Whether Progress's conduct was negligent;

l. Whether Progress's conduct was negligent *per se;*

m. Whether Progress's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

n. Whether Progress breached implied contracts with Plaintiffs and Class members;

o. Whether Progress breached third-party beneficiary contracts with Plaintiffs and Class members'

p. Whether Progress was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class members;

q. Whether Progress invaded the Privacy of Plaintiffs and Class members;

r. Whether Progress failed to provide accurate and complete notice of the Data Breach in a timely manner; and

s. Whether the Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

129. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the Class members because Plaintiffs' Personal Information, like that of every Class member, was accessed and exposed in the Data Breach.

130. **Adequacy of Representation under Federal Rule of Civil Procedure 23(a)(4)**. Plaintiff**s** will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

131. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** Progress has engaged in a common course of conduct toward Plaintiffs and the Class members, in that all Plaintiffs' and the Class members' data at issue here was stored by Progress and accessed and exposed during the Data Breach. The common issues arising from Progress's conduct affecting Class members, as described *supra,* predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

132. **Superiority under Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Progress. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

133. **Declaratory and Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2)**. Progress has acted on grounds that apply generally to the Plaintiffs and the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief

are appropriate on a Class-wide basis. Progress failed to take actions to safeguard Plaintiffs' and Class members' Personal Information such that injunctive relief is appropriate and necessary.

134. **Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4)**. In the alternative, this litigation can be brought and maintained a class action with respect to particular issues, such as Progress's liability with respect to the foregoing causes of action.

CAUSES OF ACTION

135. Plaintiffs bring these causes of action on behalf of the Nationwide Class, the California Subclass, and the Colorado Subclass, as defined herein.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1: NEGLIGENCE
On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

136. Plaintiffs incorporate by reference and re-allege the allegations contained in all preceding paragraphs of this Complaint.

137. Progress collected Plaintiffs' and Class members Personal Information, including PII and PHI.

138. Plaintiffs and Class members had a reasonable expectation that their Personal Information, including PII and PHI, would be securely maintained and not easily accessible to, or exposed by cybercriminals.

139. Plaintiffs and Class members had a reasonable expectation that in the event of a data breach, Progress would provide timely and adequate notice and would properly identify what Personal Information was exposed during a data breach so that Plaintiffs, Class and Subclass members could take prompt and appropriate steps to safeguard their identities.

140. As a Business Associate of Covered Entities, Progress had a duty to employ reasonable security measures to Plaintiffs' and Class members' patient data under HIPAA Privacy

Rule 45 C.F.R. Part 160 and Part 164 Subparts A and E, and under HIPAA Security Rule 45 C.F.R Part 160 and Part 164 Subparts A and C.

141. Progress had a duty to employ reasonable security measures to Protect Plaintiffs' and Class members' Personal Information under Section 5 of the Federal Trade Commission Act, 15. U.SC. § 45 ("FTCA"), which prohibits "unfair practices in or affecting commerce," including the unfair practice of failing to use reasonable measures to protect confidential data.

142. Progress, as a sophisticated software company that collects sensitive Personal Information, including PII and PHI, from consumers and patients and likewise stores, maintains, distributes, shares, and sells that data for profit, has a contractual duty to protect that Personal Information and in the event of a Data Breach, to promptly and to adequately notify Plaintiffs and Class members that their Personal Information has been accessed and disclosed by an unauthorized party, CL0P.

143. Progress, as a sophisticated software company that collects sensitive Personal Information from consumers and patients such as Plaintiffs and Class members, and likewise stores, maintains, distributes, shares, and sells that data for profit, has a duty arising independently from any contract to protect that information and in the event of a Data Breach, to promptly and adequately notify Plaintiffs and Class members.

144. Progress, as a sophisticated software company that contracts with companies that collect sensitive Personal Information from consumers and patients such as Plaintiffs and Class members, and likewise stores, maintains, distributes, shares, and sells that data knows that Plaintiffs and Class members are the primary beneficiary of that contract and therefore has a third party contractual duty to protect that Personal Information and in the event of a Data Breach, to

promptly and to adequately notify Plaintiffs and Class members that their Personal Information has been accessed by an unknown and unauthorized party and exposed on a hacking forum.

145. Progress, as a company that purports to be committed to protecting Personal Information owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, including email servers, and the personnel responsible for them, adequately protected and safeguarded the Personal Information of the Plaintiffs and the Class members.

146. Likewise, as the collector and keeper of Plaintiffs and Class members' Personal Information, Progress had a special duty to of Plaintiffs and Class members to promptly and adequately provide notice of the Data Breach so as to allow Plaintiffs and Class members to take prompt and appropriate steps to safeguard their Personal Information, their identities, and their credit.

147. Progress had a common law duty to prevent foreseeable harm to others. Plaintiffs and Class members were the foreseeable and probable victims of its inadequate security practices. It was foreseeable that Plaintiffs and Class members would be harmed by Progress's failure to protect their Personal Information because hackers are known to routinely attempt to seal such information and use if for criminal purposes.

148. Progress knew or should have known that the Plaintiffs, and Class members were relying on Progress to adequately safeguard and maintain their Personal Information.

149. Progress publicly acknowledged Plaintiffs and Class members' reliance on Progress's duty to safeguard their Personal Information it its 2022 annual report.

150. Progress breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs' and Class members' data. The specific negligent acts and omissions committed by Progress include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Personal Information;

b. Failing to adequately monitor the security of its network, systems and servers;

c. Failing to ensure that its products were securely coded and adequately scanned for vulnerabilities;

d. Failing to have in place policies and procedures to mitigate the harm caused by a Data Breach;

e. Failing to detect in a timely manner that Class member's Personal Information had been accessed by an unauthorized party and exposed on the dark web;

f. Failing to timely notify Class members about the Data Breach so Class members could take appropriate steps to promptly mitigate the potential for additional injuries such as fraud, identity theft, and other damages.

151. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT 2: NEGLIGENCE *PER SE*
On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

152. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-151 of this Complaint.

153. In addition to the common law and special relationship duties alleged herein, Progress also owed a duty to safeguard Plaintiffs' and Class members' Personal Information by statute.

154. Progress's duty of care to use reasonably security measures arose as a result of the special relationship that existed between Progress and consumers, recognized by laws and regulations, including, but not limited to HIPAA, the FTC Act, and common law. Progress was best positioned to ensure its network and systems were sufficiently secure to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a data breach.

155. Progress's duty to use reasonably security measures to protect patient's Personal Information including PHI under HIPAA required Progress implement administrative, physical and technical safeguards to protect the security of such information in accordance with 45 C.F.R. Parts 160, 164.

156. Progress's duty to use reasonable security measures to protect consumer's confidential information arises under Section 5 of the Federal Trade Commission Act, 15. U.SC. § 45 ("FTCA"), which prohibits "unfair practices in or affecting commerce," including the unfair practice of failing to use reasonable measures to protect confidential data.

157. Progress's duty to use reasonable care in protecting Personal Information arose not only as a result of the statutes and regulations described above, but also because Progress is bound by industry standards to protect confidential Personal Information.

158. Progress breached that duty, which, as discussed herein, caused Plaintiffs and Class members injuries, for which they are entitled to damages.

159. As a direct and proximate result of Progress's negligent conduct, Plaintiffs and Class members have suffered injuries and are entitled to nominal, compensatory, consequential and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT 3: GROSS NEGLIGENCE
On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

160. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-151 of this Complaint.

161. Progress knew that it was protecting the most sensitive Personal Information about Plaintiffs and Class members that exists, i.e., healthcare information, which can impact any area of an individual's life, *e.g.*, housing, employment, benefits, and education.

162. Progress's failure to keep this Personal Information, including PII and PHI, safe was grossly negligent, as Progress was aware of the grave consequences of not keeping this Personal Information secure.

163. As a result of Defendant's gross negligence, Plaintiffs and Class members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT 3: BREACH OF IMPLIED CONTRACT
On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

164. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-151 of this Complaint.

165. Progress acquired and maintained Personal Information belonging to Plaintiffs and Class members that Progress received either directly or from its healthcare provider customers.

166. When Plaintiffs and Class members paid money and provided their Personal Information to their doctors and/or other healthcare providers, either directly or indirectly, in

exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and clinical laboratories, including Progress.

167. Plaintiffs and Class members entered into implied contracts with Progress under which Progress agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members that their Personal Information had been breached, accessed by an unknown and unauthorized party, and exposed on a hacking forum.

168. Plaintiffs and Class members were required to indirectly deliver their Personal Information to Progress as part of the process of obtaining services provided by Progress. Plaintiffs and Class members paid money, or money was paid on their behalf, to Progress in exchange for services.

169. Progress accepted possession of Plaintiffs' and Class members' Personal Information for the purpose of indirectly providing services to Plaintiffs and Class members.

170. In accepting such information and payment for services, Progress entered into an implied contract with Plaintiffs and the other Class members whereby Progress became obligated to reasonably safeguard Plaintiffs' and the other Class members' Personal Information.

171. Alternatively, Plaintiff and Class members were the intended beneficiaries of data protection agreements entered into between Progress and healthcare providers.

172. Progress's implied promise of confidentiality includes consideration beyond those preexisting general duties owed under HIPAA, the FTC Act, or other state of federal regulations. The additional consideration also included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

173. Progress's implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Personal Information also protect the confidentiality of

that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to authorized, qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the Personal Information against data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

174. Plaintiffs and the Class members would not have entrusted their Personal Information to Progress in the absence of such an implied contract.

175. Had Progress disclosed to Plaintiffs and Class members (or their physicians) that Progress did not have adequate computer systems, information technology security tools, and security practices to secure sensitive data, Plaintiffs and the other Class members would not have provided their Personal Information to Progress (or to their physicians to provide to Progress).

176. Progress recognized that Plaintiffs' and Class members' Personal Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and to the other Class members.

177. Plaintiffs and the other Class members fully performed their obligations under the implied contracts with Progress. Progress breached the implied contract with Plaintiffs and the other Class members by failing to take reasonable measures to safeguard their Personal Information as described herein.

178. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT 4: BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

179. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-151 of this Complaint.

180. Upon information and belief, Progress entered into nearly identical contracts with its customers to provide secure file transfer services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the Personal Information that was entrusted to it.

181. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Personal Information that Defendant agreed to receive and protect through its services.

182. Thus, the benefit of collection and protection of the Personal Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class members were direct and express beneficiaries of such contracts.

183. Progress knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

184. Progress breached its contracts with customers by, among other things, failing to adequately secure Plaintiffs' and Class members' Personal Information, and, as a result, Plaintiff and Class Members were harmed by Progress's failure to secure their Personal Information.

185. As a direct and proximate result of Progress's breach, Plaintiffs and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Personal Information; (vii) future costs of identity theft

monitoring; (viii) and the continued risk to their Personal Information, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Personal Information.

186. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

187. Plaintiffs and Class members are also entitled to injunctive relief requiring Progress to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members. sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Personal; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Personal, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Personal Information.

188. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

189. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT 5: UNJUST ENRICHMENT

On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

190. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-151 of this Complaint.

191. This count is pleaded in the alternative to any breach of contract claim.

192. Upon information and belief, Progress funds its data security measures entirely from general revenue, including from money Progress makes based upon protecting Plaintiffs' and Class members' Personal Information.

193. There is a direct nexus between money paid to Progress and the requirement that Progress keep Plaintiffs' and Class members' Personal Information confidential and protected.

194. Plaintiffs and Class members indirectly paid Progress a certain sum of money, which was used to fund data security via contracts with Progress.

195. As such, a portion of the payments made by or on behalf of Plaintiffs and Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Progress.

196. Protecting data from Plaintiffs and from Class members is integral to Progress's business. Without Class members' data, Progress would not be able to provide its customers with software products and solutions, thus compromising Progress's core business.

197. Plaintiffs' and Class members' data has monetary value, and Plaintiffs' and Class members directly and indirectly conferred a monetary benefit on the Progress. Plaintiffs and Class members indirectly conferred a monetary benefit on Progress by purchasing goods and/or services from entities that contracted with Progress, and from which Progress received compensation to

protect certain data. Plaintiffs and Class members directly conferred a monetary benefit on Progress by supplying Personal Information, which has value, from which value Progress derives its business value, and which should have been protected with reasonable and adequate data security.

198. Progress knew that Plaintiffs and Class members conferred a benefit which Progress accepted. Progress profited from these transactions and used Plaintiffs' and Class members for Progress's business purposes.

199. Progress enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Progress instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Progress's failure to provide the requisite security.

200. Under the principles of equity and good conscience, Progress should not be permitted to retain the money belonging to Plaintiffs and Class members, because Progress failed to implement appropriate, reasonable, and adequate data management and security measures that are mandated by industry standards.

201. acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

202. If Plaintiff and Class members knew that Progress had not secured their Personal Information, they would not have agreed to provide their Personal Information to Progress.

203. Plaintiff and Class members have no adequate remedy at law.

204. As a direct and proximate result of Progress's conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their Personal Information is used; (iii) the access, compromise, publication, exposure, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Personal Information, which remain in Progress's possession and is subject to further unauthorized disclosures so long as Progress fails to undertake reasonable appropriate and adequate measures to protect Personal Information in its continued possession; (vii) loss or privacy from the unauthorized access and exposure of their Personal Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information accessed by an unknown and unauthorized party and exposed as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

205. As a direct and proximate result of Progress's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

206. Progress should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Progress should be compelled to refund the amounts that Plaintiffs and Class members overpaid for Progress's services.

COUNT 6: INVASION OF PRIVACY

On behalf of Plaintiffs and the Nationwide Class Under Massachusetts Law

207. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-151 of this Complaint.

208. Plaintiffs and Class members have a legally protected privacy interest in their Personal Information, which is and was collected, stored, and maintained by Progress, and they are entitled to the reasonable and adequate protection of their Personal Data against foreseeable unauthorized access, as occurred with the Data Breach.

209. Plaintiffs, Class and Subclass members reasonably expected that Progress would protect and secure their Personal Information from unknown and unauthorized parties and that their Personal Information would not be accessed and disclosed to any unauthorized parties or for any improper purpose.

210. Progress unlawfully invaded the privacy rights of Plaintiffs and Class members by engaging in the conduct described above, including by failing to protect their Personal Information by permitting an unauthorized and unknown party to access and expose that Personal Information. Likewise, Progress further invaded the privacy rights of Plaintiffs, Class members, and permitted criminals to invade the privacy rights of Plaintiffs and Class members, by unreasonably and by delaying disclosure of the Data Breach, and failing to properly identify what Personal Information had been accessed and exposed by an unknown and unauthorized party.

211. . This invasion of privacy resulted from Progress's failure to properly secure and maintain Plaintiffs' and Class members' Personal Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

212. Plaintiffs' and Class members' Personal Information is the type of sensitive information that one normally expects will be protected from exposure by the very entity charged

with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class members' Personal Information, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

213. The disclosure of Plaintiffs and Class members' Personal Information to unknown and unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

214. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class members' Personal Information was without their consent, and in violation of various statutes, regulations and other laws.

215. Plaintiffs, the Class and Subclasses members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 7: CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*

216. The California Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-215, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

217. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81 .5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the

information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

218. Progress is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(l), about Plaintiff and California Subclass members.

219. Progress is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code§ 1798.99.80.263

220. Businesses that own or license computerized data that includes personal information, including SSNs, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code§ 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code§ 1798.82. *Id.*

221. Progress is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

222. Plaintiff's and California Subclass members' Personal Information includes "personal information" as covered by Cal. Civ. Code§§ 1798.81.S(d)(l), 1798.82(h).

223. Because Progress reasonably believed that Plaintiff and California Subclass members' Personal Information was acquired by unauthorized persons during the Data Breach, Progress had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

224. Progress failed to fully disclose material information about the breach.

225. By failing to disclose the Data Breach in a timely and accurate manner, Progress violated Cal. Civ. Code § 1798.82.

226. As a direct and proximate result of Progress's violations of the Cal. Civ. Code§§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

227. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 8: CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code§§ 17200, *et seq.*

228. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-215, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair competition.

229. Progress is a "person" as defined by Cal. Bus. & Prof. Code §17201.

230. Progress violated Cal. Bus. & Prof. Code§§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

231. Progress's "unfair" and "deceptive" acts and practices include:

a. Progress failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Progress failed to identify foreseeable security risks, remediate identified security risks, and

adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

b. Progress's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws including California's Consumer Legal Remedies Act ("CLRA"), Cal Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Confidentiality of Medical Information Act ("CMIA"), Cal Civ. Code § 56.26(b), and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Progress's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Progress's inadequate security, consumers could not have reasonably avoided the harms that Progress caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

232. Progress has engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.,* the CLRA, Cal. Civ. Code §§ 1780, *et seq.,* 15 U.S.C. § 680, *et seq.,* the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

233. Progress's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.,* the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.,* HIPAA**,** 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the CLRA, Cal. Civ. Code§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b);

f. Failing to timely and adequately notify the Customers, Plaintiffs, and California Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Personal Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the CLRA, Cal. Civ. Code§ 1780, *et seq.,* the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.,* HIPAA, 42 U.S.C. § 1320d, COPP A, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

234. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's data security and ability to protect the confidentiality of consumers' Personal Information.

235. Progress's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the California Subclass members, into believing that their Personal Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

236. As a direct and proximate result of Progress's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information, including but not limited to the diminishment of their present and future property interest in their Personal Information and the deprivation of the exclusive use of their Personal Information.

237. Progress acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights.

238. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Progress's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure§ 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 9: CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code§§ 1750, *et seq.*

239. The California Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-215, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf

of all other natural persons whose Personal Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer legal remedies.

240. The Consumers Legal Remedies Act, Cal. Civ. Code§§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

241. Progress is a "person" as defined by Civil Code § § 17 61 (c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

242. Plaintiffs and the California Class are "consumers" as defined by Civil Code §§ 17 61 (d) and 1770, and have engaged in a "transaction" as defined by Civil Code § § 17 61 (e) and 1770.

243. Progress's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

e. Progress violated Civil Code § 1770, in the following ways:

f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code§ 56.36(b), which was a direct and proximate cause of the Data Breach;

i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code§ 56.36(b);

k. Failing to timely and adequately notify the Customers, Plaintiffs, and California Subclass members of the Data Breach;

l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Personal Information; and

n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.,* HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

244. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's data security and ability to protect the confidentiality of consumers' Personal Information.

245. Progress's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Personal Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

246. Had Progress disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Progress would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Progress was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs, the Class, and the California Subclass. Progress

accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Progress held itself out as maintaining a secure platform for Personal Information data, Plaintiffs, the Class, and the California Subclass members acted reasonably in relying on Progress's misrepresentations and omissions, the truth of which they could not have discovered.

247. As a direct and proximate result of Progress's violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information, including but not limited to the diminishment of their present and future property interest in their Personal Information and the deprivation of the exclusive use of their Personal Information.

248. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT 12: CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civil Code § 56, *et seq.*

249. Plaintiff, individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-215, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

250. The California's Confidentiality of Medical Information Act ("CMIA") prohibits among other things, unauthorized disclosure of private medical information. Cal. Civ. Code§§ 56, *et seq.*

251. Plaintiff provided PHI to Progress's customer which is a "health care practitioner" and is a "provider of health care" as defined by Cal. Civ. Code§ 56.05(j).

252. Plaintiff is a "patient" as defined by Cal. Civ. Code§ 56.05(k).

253. Progress is a "provider of health care" subject to the CMIA because it is a "business that offers software or hardware to consumers, ... that is designed to maintain medical information" in order to make the information available to an individual or Customer to which Plaintiff provided her PHI. Cal. Civ. Code§ 56.06(b).

254. Progress stored in electronic form on its computer system Plaintiffs "medical information" as defined by Cal. Civ. Code § 56.05(j).

255. Progress's systems were designed, in part, to make medical information available to Customers by providing cloud-based computing solutions through which those organizations could store, access, and manage consumers' medical information, including but not limited to diagnosing, treating, or managing consumers' medical conditions.

256. Plaintiff did not provide Progress authorization nor was Progress otherwise authorized to disclose Plaintiffs medical information to an unauthorized third-party.

257. As described throughout this Complaint, Progress negligently maintained, disclosed and released Plaintiff and the California PHI Subclass members' medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or

employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

258. As a direct and proximate result of Progress's negligence, it disclosed and released Plaintiff and the California PHI Subclass members' medical information to an unauthorized third-party.

259. Progress's unauthorized disclosure of medical records has caused injury to the Plaintiff and the California PHI Subclass.

260. Upon information and belief, Plaintiff's confidential medical information was viewed by an unauthorized third party.

261. Accordingly, Plaintiff, individually and on behalf of members of the California PHI Subclass, seek to recover actual, nominal (including $1000 nominal damages per disclosure under§ 56.36(b)), and statutory damages (including under§ 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 13: COLORADO SECURITY BREACH NOTIFICATION ACT
Colo. Rev. Stat.§§ 6-1-716, *et seq.*

262. The Colorado Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-215, as if fully alleged herein. This claim is brought individually under the laws of Colorado and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

263. Progress is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat.§§ 6-1-716(1) and 6-1-716(2).

264. 785. Plaintiff's and Colorado Subclass members' Personal Information includes "Personal Information" as covered by Colo. Rev. Stat.§§ 6-1-716(1) and 6-1-716(2).

265. Progress is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security program in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

266. Because Progress was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat.§ 6-1-716(2).

267. By failing to disclose the Data Breach in a timely and accurate manner, Progress violated Colo. Rev. Stat.§ 6-1-716(2).

268. As a direct and proximate result of Progress's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered and will continue to suffer damages, as described above.

269. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT 14: COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, *et seq.*

270. The Colorado Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-215, as if fully alleged herein. This claim is brought individually under the laws of Colorado and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

271. Progress is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

272. Progress engaged in "sales" as defined by Colo. Rev. Stat.§ 6-1-102(10).

273. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Progress or successors in interest to actual consumers.

274. Progress engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat.§ 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Progress knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised; and

d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

e. Progress's deceptive trade practices include:

f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Colorado Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Colorado Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

k. Failing to timely and adequately notify customers, Plaintiff, and Colorado Subclass members of the Data Breach;

l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Colorado Subclass members' Personal Information; and

m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

275. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's data security and ability to protect the confidentiality of consumers' Personal Information.

276. Progress's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Colorado Subclass members, that their Personal Information was not exposed and misled Plaintiffs and the Colorado Subclass members into believing they did not need to take actions to secure their identities.

277. Progress intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

278. Had Progress disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Progress would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Progress was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff's, the Class member's, and the Colorado Subclass member's. Progress accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Progress held itself out as maintaining a secure platform for Personal Information, Plaintiff, the Class members, and the Colorado Subclass members acted reasonably in relying on Progress's misrepresentations and omissions, the truth of which they could not have discovered.

279. Progress acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff's and Subclass members' rights.

280. As a direct and proximate result of Progress' s deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

281. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Progress's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs request for judgement as follows:

(a) For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class and the Colorado Subclass;

(b) For equitable relief enjoining Progress from engaging in the wrongful conduct complained of herein pertaining to the misuse and disclosure of Plaintiffs' Class and Subclass members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs, Class and Subclass members, or to mitigate further harm;

(c) For equitable relief compelling Progress to devise and employ appropriate methods and policies with respect to consumer and patient data collection, storage, and protection, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

(d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Progress's wrongful conduct;

(e) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

(f) For an award of punitive damages, as allowable by law;

(g) Ordering Progress to pay for not less than 10 years of three bureau credit monitoring, identity theft monitoring, and identity theft insurance for Plaintiffs, Class and Subclass members;

(h) For an award of attorneys' fees and costs, and any other expense, including reasonable expert witnesses fees;

(i) Pre- and post-judgement interest on any amounts awarded;

(j) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 20th day of October, 2023

Respectfully Submitted,

/s/ Donna M. Evans
Donna M. Evans
COHEN MILSTEIN SELLERS AND TOLL, PLLC
769 Centre Street
Suite 207
Boston, MA 02130
Telephone: (617) 858-1990
devans@cohenmilstein.com

Douglas McNamara*
Blake R. Miller*
COHEN MILSTEIN SELLERS AND TOLL, PLLC
1100 New York Avenue NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699
dmcnamara@cohenmilstein.com
brmiller@cohenmilstein.com

Claire Torchiana*
COHEN MILSTEIN SELLERS AND TOLL PLLC
88 Pine Street, 14th Floor
New York, NY 10005
Telephone: (212) 220 2914
Facsimile: (212) 838 7745
ctorchiana@cohenmilstein.com

Amy Keller*
James Ulwick
DICELLO LEVITT LLP
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60610
Telephone: (312) 214-7900
akeller@dicellolevitt.com
julwick@dicellolevitt.com

Corban Rhodes*
DICELLO LEVITT LLP
485 Lexington Avenue
Suite 1001
New York, New York 10017
crhodes@dicellolevitt.com

*Pending Admission Pro Hac Vice